Best Practices for Application Risk Management

Mike Puglia, Director

VERACODE

Agenda

1. State of Software Security
2. Compliance Initiatives
3. Moving to Application Risk Management

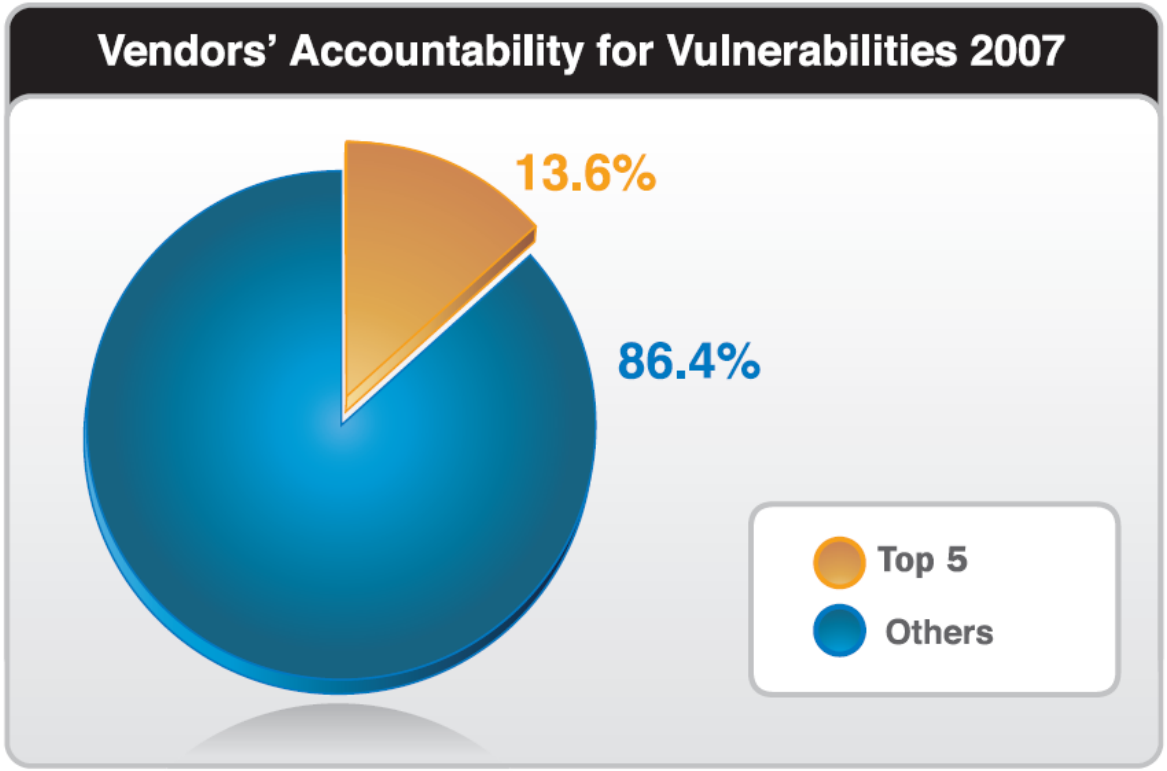
Application Security: View From the Trenches

- Did I cause this?
  - Confessions of a reformed Product Manager
- 15+ Years of Software Development (Before I came to Veracode)
  - Huge pressures on features and schedules
  - Little organizational knowledge around application security
  - Few customer requests

Myth – All Vulnerabilities are from Large Software Vendors

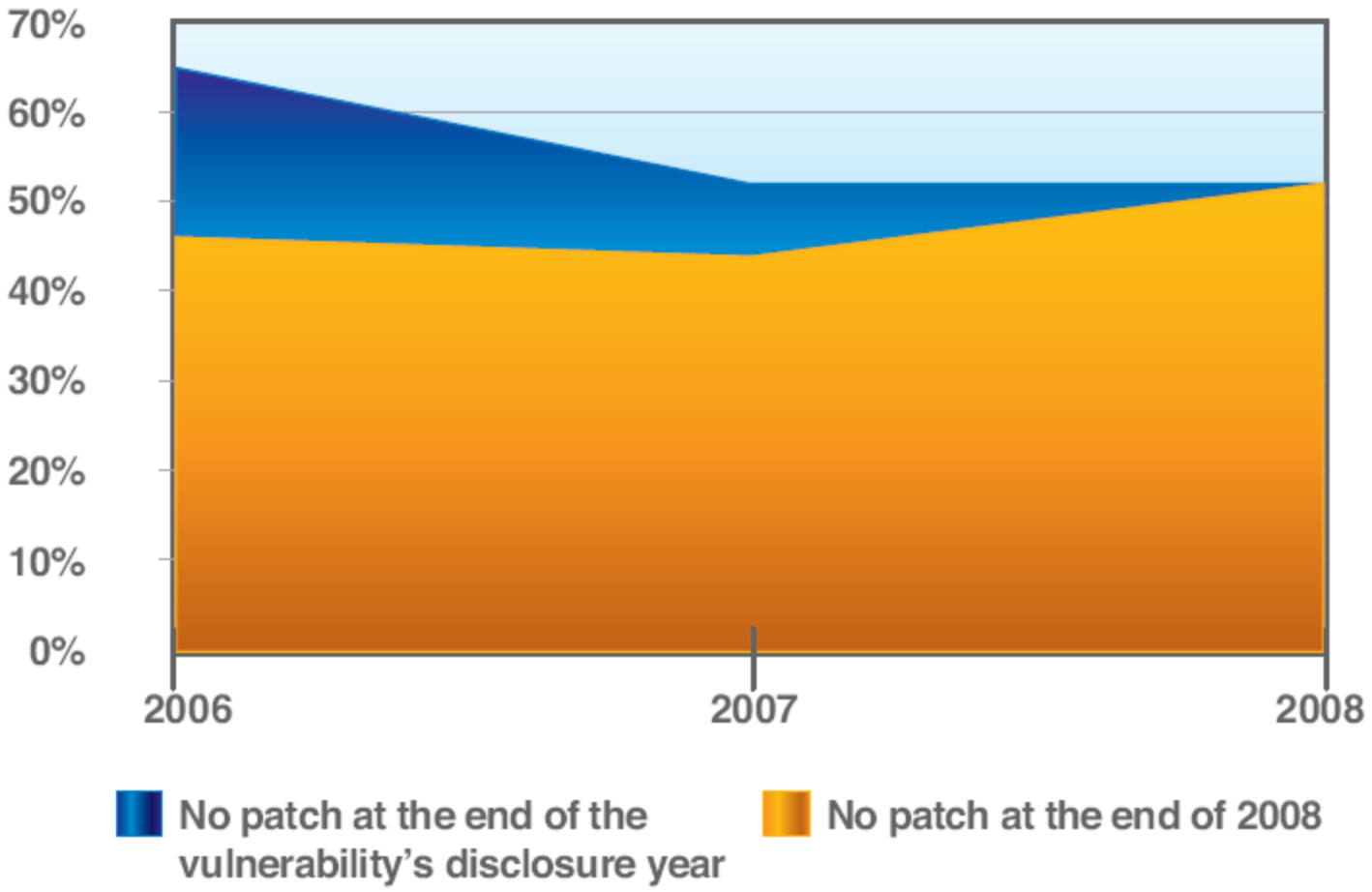
Vendor	Vulnerabilities Reported in 2007
Microsoft	238
Apple	207
Oracle	183
IBM	137
Cisco	113

Source: IBM X-Force 2007 Security Trends Report



"Microsoft executives said they were pleased with the progress made since the company was shaken by a series of destructive programs that spread rapidly around the world over the Internet beginning in 2003. But they said that unless software development practices change throughout the industry, any improvements in the security of Windows would be meaningless." – New York Times, Nov 3, 2008

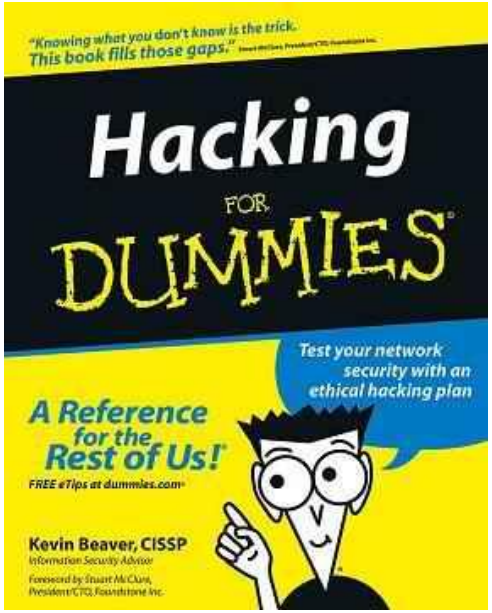
Even Disclosed Vulnerabilities Go Un-Patched



Source: IBM X-Force 2008 Vulnerability Report

Houston, We Have a Problem

- ISV Customer Base
  - » Large Fortune 500 Enterprises
  - » Financial Services
  - » Government
- One customer required security information as part of an RFP
- One customer tested (black box) against the admin web interface
- Two independent security researchers found issues
- Results
  - » “Firefighting”
  - » Lack of remediation knowledge
  - » Difficulty in justifying application security spend
  - » FIPS140-2 and other certifications delayed fixes

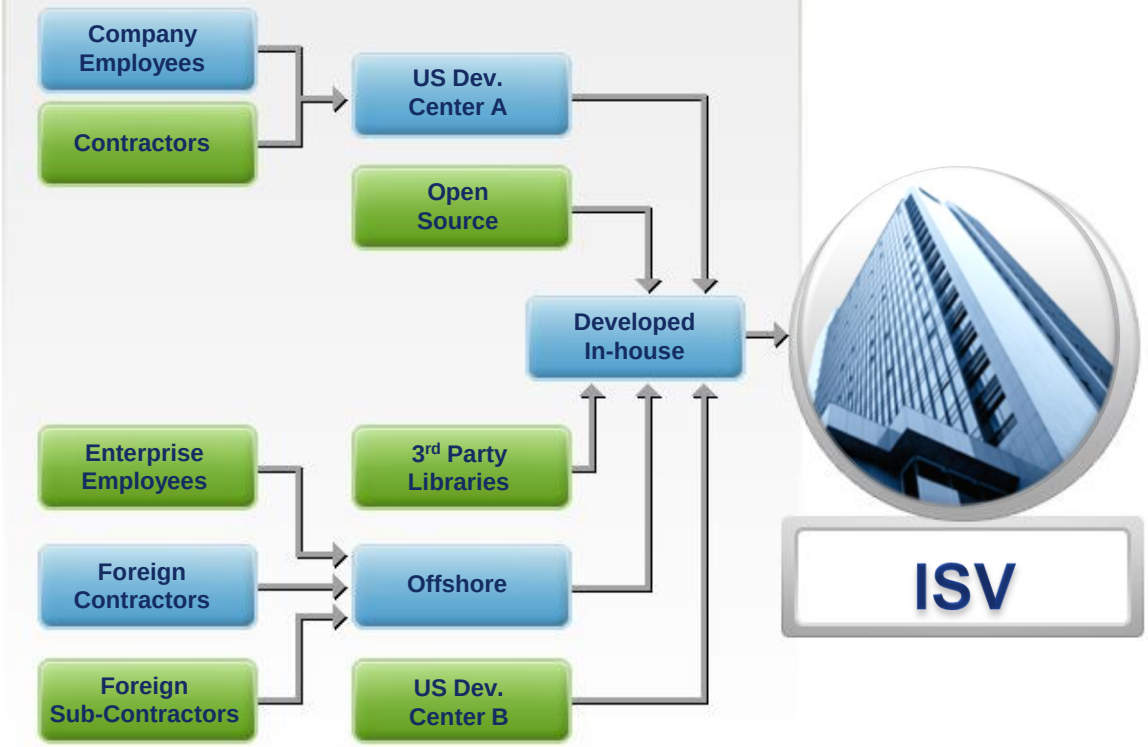


Real-World Examples: Best Intentions Gone Bad

Wargames (1983)

Application Development and Procurement Have Become Increasingly Distributed and Complex

Development Process



ISV

- Rapidly growing ISV in highly security-sensitive marketplace
- Pressure from customer to prove software quality
- Fast time to market requirements with little internal security expertise

Enterprise

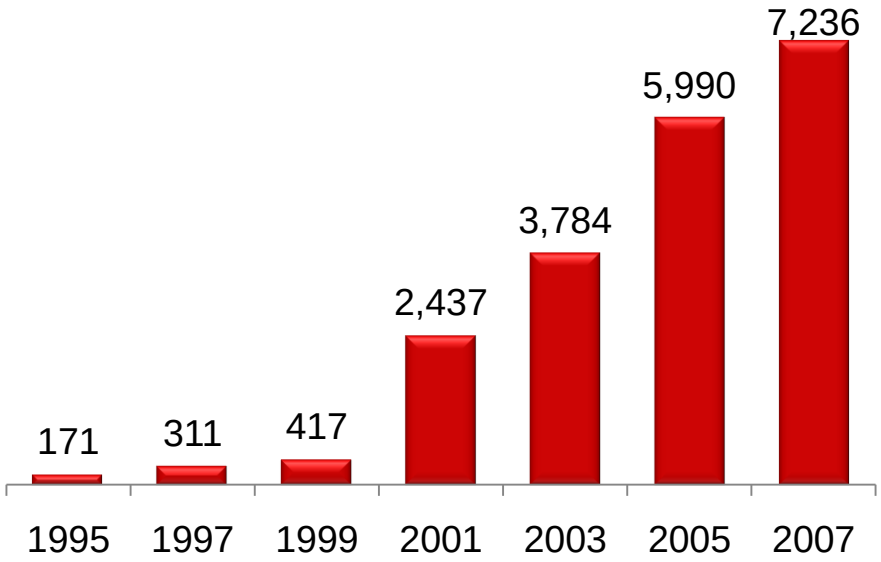
- Contracts focus on features and functions
- Price and delivery are key requirements
- Security is checked “after the fact” if at all
- Most requirements surround network security (ports, security functions)

The Unbounded Risk of Insecure Software

Applications are the "Attack Surface" Leading to the Data

State of Software Industry:

- Over $350 Billion in off-the-shelf, internally developed and outsourced software produced or sold each year
- This is the **world's largest manufacturing industry** with no uniform standards or insight into security, risk or liability of the final product
- Over 7,000 new vulnerabilities reported last year alone



Source: CERT, 2008

Agenda

1. State of Software Security
2. Compliance Initiatives
3. Moving to Application Risk Management

Drivers for Application Risk Management

Regulations and Standards

- PCI-DSS & PA-DSS
- OCC Bulletin 2008-16
- DISA
- FISMA/HIPAA/GLBA/SOX
- OWASP Top 10
- SANS Top 25

Operations and Customers

- Information theft
- Information denial
- Service Availability
- Brand risk and trust
- Redundant Audits
- High remediation cost

Regulatory Compliance, Standards & Frameworks
Adapting to Application Security Challenges

Comptroller of the Currency Administrator of National Banks US Department of the Treasury OCC 2008-16 **OCC BULLETIN**	*"All applications, whether **internally developed**, **vendor-acquired** or **contracted** for, should be subject to appropriate security risk assessment and mitigation processes."*
PCI Security Standards Council **PCI Data Security Standard (PCI DSS/PA-DSS)**	*Confirm that all payment application components are reviewed by an organization that specializes in application code security.*
MAS Monetary Authority of Singapore **Banking and Technology Risk Management Guidelines**	*Perform application security review using a combination of code review, stress loading and exception testing to identify insecure coding techniques and systems vulnerabilities.*
SANS **OWASP Top 10** **SANS Top 25**	*Indentifies Top Vulnerabilities and Dangerous Programming Errors – Enabling Procurement Language and Requirements*

OCC Bulletin 2008-16
A Blueprint for Application Security & Compliance

- Application security is critical
  - » Vulnerabilities in applications increase operational and reputation risk
- All applications are “in-scope”
  - » Internally developed
  - » vendor-acquired
  - » contracted for (outsourced)
  - » Both web and non-web applications
- Security responsibility lies with the bank
  - » Regardless of the source of the app (internal or 3rd party)
- Validate independently the security of the application.

Application Security Vulnerabilities
OCC, PCI & Minimum Due Care

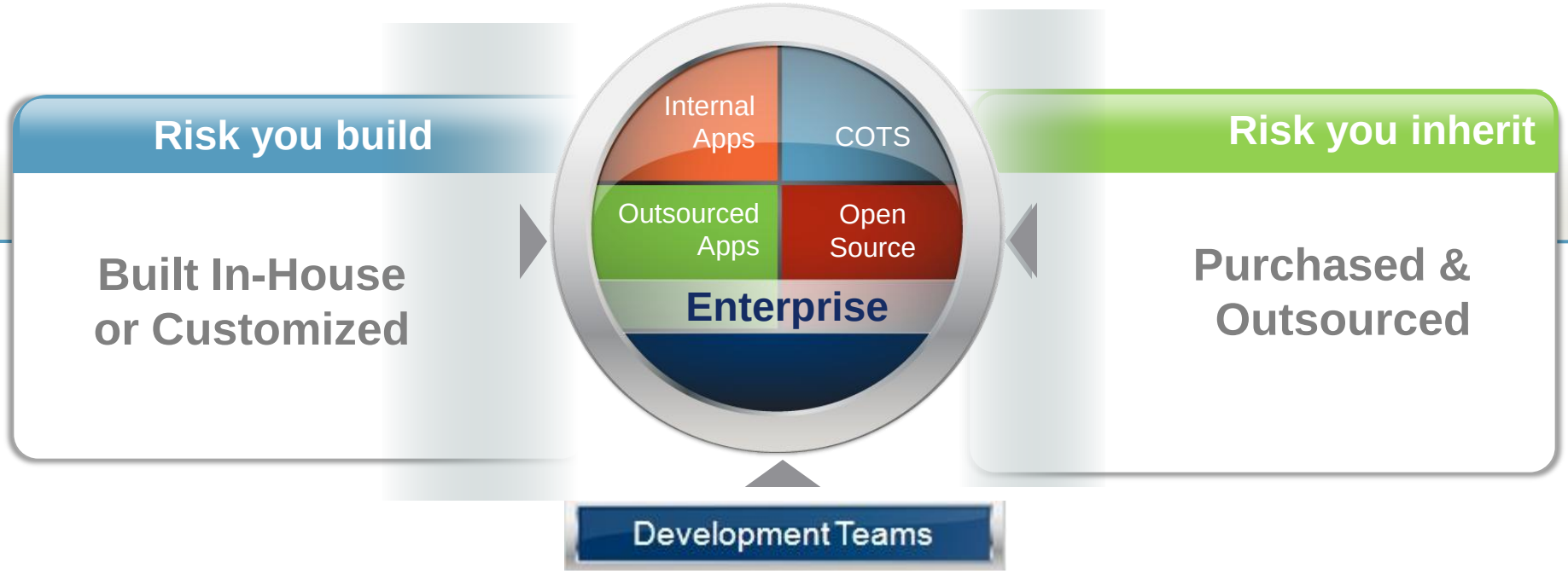
OCC Bulletin & PCI Reference OWASP Top 10 Vulnerability List as an example of minimum due care when evaluating application security risks

- Cross-Site Scripting (XSS)
- Injection Flaws (SQL Injection)
- Malicious File Execution
- Insecure Direct Object Reference
- Cross Site Request Forgery (CSRF)
- Information Leakage
- Broken Authentication and Session Management
- Insecure Cryptographic Storage
- Insecure Communication
- Failure to Restrict URL Access

Agenda

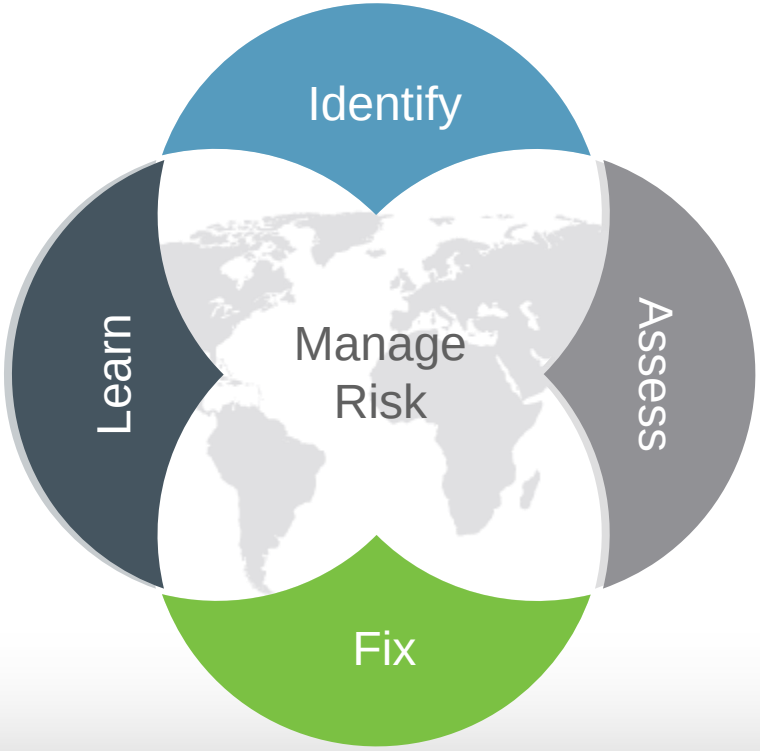
1. State of Software Security
2. Compliance Initiatives
3. Moving to Application Risk Management

All Application Security Risk Has Two Root Causes



Application
Portfolio
Transparency

Application Risk Management



Best Practices Framework

- **Identify** applications, assign business criticality, set security policy
- **Assess** applications against security policy
- **Fix** problems, remediated code, meet policy
- **Learn** from findings, formal training and competency testing

Software Risk Analysis

Assigning Application Assurance Levels

Assurance Level	Description
Very High	Mission critical for business/safety of life and limb on the line
High	Exploitation causes serious brand damage and financial loss with long term business impact
Medium	Applications connected to the internet that process financial or private customer information
Low	Typically internal applications with non-critical business impact
Very Low	Applications with no material business impact

U.S. Govt. OMB Memorandum M-04-04

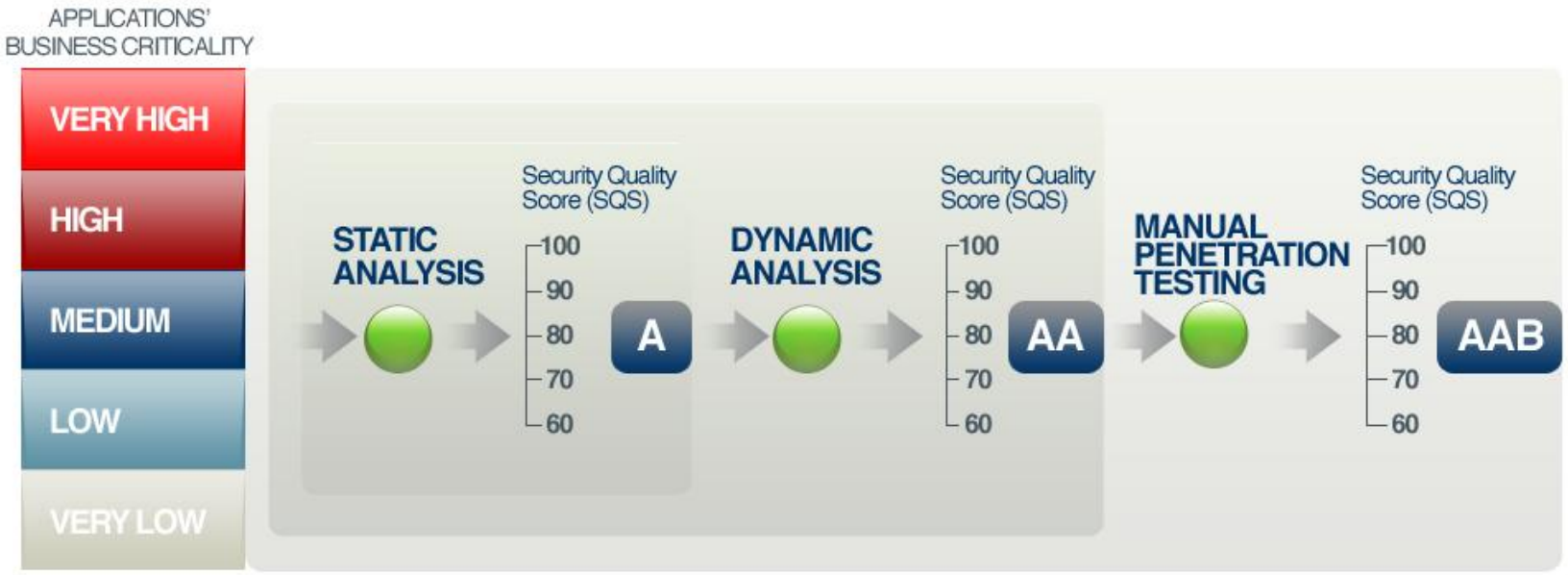
Implement Measurable Standardized Metrics

- Independent ratings based on industry standards enables better decision-making (CWE, CVSS, NIST)
- Eliminate the headaches associated with normalizing output from multiple testing techniques and vendors
- A common language to compare internally and externally developed code
- Ratings benefit both the Enterprise and the Provider

Gartner

"CVSS support should be a requirement for all vulnerability assessment procurements, and enterprises should urge all IT suppliers to use CVSS scoring when disclosing vulnerabilities."

–John Pescatore, Gartner



Embed Security Acceptance Testing into Contracts

- Software contracts typically focus on features, functions, maintenance and delivery timeframes
- Enterprises can embed security language into contracts
  - New purchases or maintenance renewals are optimal times to introduce security
- Security testing is <u>not</u> functional testing, the contract should specify:
  - Specific security measures (for example, code review, dynamic testing, penetration testing)
  - Specific tools that should be used for testing
  - Acceptance thresholds for testing
  - Vulnerability correction rules

SANS Top 25 Most Dangerous Programming Errors

New Application Security Procurement Language

DTCC

The Depository Trust & Clearing Corporation

SANS

Application Security Procurement Language

New York Plans Application Security Program

Developers must straighten up and fly right if they want to do business with the Empire State.

Authors:
Will Pelgrin, CSO New York State
Jim Routh, CISO, Depository Trust and Clearing Corporation

Transparency: Cyber UL & Independent Assessments

- Work collaboratively with software providers
- Trusted 3rd party provides transparency and unbiased analysis based on industry standards (SANS, CWE, etc…)
- Independent Verification & Validation (IV&V)
  - » Meets auditing standards
  - » Segregation of Duties
  - » Strong proof of a security control
- Liability & Costs
  - » Enterprises may not want to take on the liability, risks and costs of analyzing source code

» Are we prepared for FIPS140-2, Common Criteria or PCI Model?

Underwriters Laboratories

Moody's Investors Service

Consumer Reports

"Rather than trying to change processes within both the bank and our vendors, Veracode's software-as-a-service model gave us rapid execution and results with minimal resources."

– Rhonda MacLean, CISO of Barclays

Leverage the Power of Community

1. Pooling the purchasing power of peer organizations to create demand for secure software
2. Vendors will react to fill a market need
3. Shared Application Risk Service
4. Creating a community
   - » User Groups
   - » Customer Advisory Boards
   - » Analysts
   - » Vendor Relations/Procurement

Q&A

contact@veracode.com
781-425-6040

VERACODE